WHAT IS CLAIMED IS:

1. A method for providing credential level change in a security architecture, the method comprising:

obtaining a first credential for a client entity and authenticating the client entity thereby;

accessing a first of plural information resources;

if the client entity is sufficiently authenticated for access to a second of the information resources, accessing the second information resource; and

otherwise,

obtaining a second credential for the client entity and authenticating the client entity thereby, the second credential sufficiently authenticating the client entity for access to the second information resource; and

thereafter accessing the second information resource,

wherein the accesses to first and second information resources are performed within a persistent session context and wherein the second credential obtaining and client entity authenticating are performed without loss of session continuity.

2. A method as in claim 1, further comprising:

issuing the client entity at least one session token for identifying the persistent session context to the security architecture.

3. A method as in claim 1, further comprising:

issuing to the client entity at least first and second session tokens, the first token after the first credential authenticating and the second token after the second credential authenticating,

wherein the first and second session tokens both correspond to the persistent session context.

4. A method as in claim 3,

wherein the client entity includes a browser operated by a principal; and

wherein the session token is cryptographically secured and encoded in cookie supplied to the browser.

5. A method as in claim 1, further comprising:
prior to the first credential obtaining, receiving a request from the client entity to access the first information resource; and
after the client entity authenticating by the first credential, issuing the client entity a session token for identifying the persistent session context to the security architecture.

6. A method as in claim 5,
wherein the access request receiving and the first information resource accessing are performed by a proxy.

7. A method as in claim 1, further comprising:
establishing the persistent session context prior to the first authenticating.

8. A method as in claim 1, further comprising:
before the authenticating by the second credential, accessing a third of the information resources,
the first credential sufficiently authenticating the client entity for access to the first and third information resources.

9. A method as in claim 1,
wherein, after the authenticating by the second credential, the client entity is sufficiently authenticated to access both the first and second information resources.

10. A method as in claim 1, embodied as a computer program product encoded by or transmitted in at least one computer readable medium selected from the set of a disk, tape or other magnetic, optical, or electronic storage medium and a network, wireline, wireless or other communications medium.

11. In a networked information environment having plural information resources with potentially differing authentication requirements, a method of providing a sign-on common to the information resources, the method comprising:

authenticating a client entity using a first credential;

issuing a session token corresponding to a session of the client entity;

allowing access using the session token to first and second, but not a third, of the information resources;

upgrading the session token after authenticating with a second credential; and

thereafter, without loss of session continuity, allowing access using the upgraded session token to the first, second and third information resources.

12. A method as in claim 11,

wherein the session token and the upgraded session token both resolve to a same session object, the same session object maintaining a consistent session state spanning the upgrading.

13. A method as in claim 11,

wherein the client entity includes a browser.

14. A method as in claim 11,

wherein the first and the second credentials are selected from a set including username password pairs, digital certificates, encrypted credentials based on asymmetric, symmetric, public, private, or secret key technologies, one-time passwords, biometric credentials based on retinal scan, voice print, or finger print, and possession based credentials embodied in smart cards, Enigma cards or keys;

the second credential corresponding to a higher trust level than the first.

15. A method as in claim 11, embodied as a computer program product encoded by or transmitted in at least one computer readable medium selected from the set of a disk, tape or other magnetic, optical, or electronic storage medium and a network, wireline, wireless or other communications medium.

16. In a networked information environment having plural authentication levels for access to one or more information resources, a method for providing a persistent session interface thereto, the method comprising:

authenticating an entity to a first authentication level and associating a unique session identifier with the entity;

after association of the unique session identifier, authenticating the entity to a second authentication level and maintaining the association of the unique session identifier with the entity; and

thereafter allowing access, using the unique session identifier, to the information resources at the second authentication level.

17. A method as in claim 16,

wherein the unique session identifier is encoded in one or more session tokens issued to the entity.

18. A method as in claim 16, further comprising:

after the authenticating to the first authentication level, accessing, using the unique session identifier, a first of the information resources at the first authentication level.

19. A method as in claim 18, further comprising:

after the authenticating to the second authentication level, accessing, using the unique session identifier, the first information resource at the second authentication level.

20. A method as in claim 16, further comprising:

after the authenticating to the second authentication level, accessing a second information resource at the second authentication level.

21. A method as in claim 16, embodied as a computer program product encoding instructions executable by a computer to perform the authenticating to first and second authentication levels and to perform the access allowing, the computer program product encoded by or transmitted in at least one computer readable medium

selected from the set of a disk, tape or other magnetic, optical, or electronic storage medium and a network, wireline, wireless or other communications medium.

22. A secure information system comprising:

plural information resources hosted on one or more servers coupled via a communication network to a client entity, the plural information resources having individualized authentication requirements; and

a log-on service common to the plural information resources, the common log-on service obtaining a first credential for the client entity, authenticating the client entity thereby, and establishing a session having a first authentication level commensurate with authentication requirements of at least one of the plural information resources,

wherein, in response to an access request requiring a second authentication level higher than the first, the common log-on service obtains a second credential for the client entity, authenticates the client entity thereby, and upgrades the session to the second authentication level without loss of session continuity.

23. An access management system providing a single sign-on for sessions that potentially include access to plural information resources having differing security requirements, the access management system comprising:

a gatekeeper including an authorization interface for determining whether a first authenticated credential associated with client entity and session is consistent with a trust level requirement for a target information resource and, if so, proxying an access thereto; and

means responsive to the gatekeeper for upgrading the session by obtaining and authenticating a second credential to allow access to the target information resource if the first authenticated credential is inconsistent with the trust level requirement, the session upgrade means maintaining session continuity across credential upgrades.

24. A computer program product encoded in computer readable media, the computer program product comprising:

log-on code executable on a first server as a log-on component to obtain one or more credentials for a client entity, the log-on component including an authentication interface for authenticating the client entity using the obtained one or more credentials; and

gatekeeper code executable on one of the first server and a second server as a gatekeeper component to receive access requests from the client entity, the gatekeeper component including an authorization interface for determining whether an authentication level is consistent with a trust level requirement for a target information resource and, if so, proxying an access thereto, and, if not, redirecting the access to the log-on component for obtaining and authenticating at least one additional credential to allow access to the target information resource.

25. The computer program product of claim 24, further comprising:

authentication code executable as an authentication component to perform the authenticating; and

authorization code executable as an authorization component to determining consistency of authentication levels with trust level requirements.

26. The computer program product of claim 24, encoded by or transmitted in at least one computer readable medium selected from the set of a disk, tape or other magnetic, optical, or electronic storage medium and a network, wireline, wireless or other communications medium.